Solving Structured Polynomial Systems and Applications to Cryptology
(Plenary Talk)

Jean-Charles Faugère

SALSA Project INRIA, Centre Paris-Rocquencourt
UPMC, Univ Paris 06, LIP6
CNRS, UMR 7606, LIP6
UFR Ingénierie 919, LIP6 Passy Kennedy
Boite Courrier 169, 4, Place Jussieu 75252 Paris Cedex 05
Jean-Charles.Faugere@inria.fr
http:/www-salsa.lip6.fr/~jcf

Algebraic Cryptanalysis

Cryptography is a collection of mathematical techniques used to secure the transmission and storage of information. A *fundamental* problem in cryptography is to *evaluate the security of cryptosystems* against the most powerful techniques. To this end, several *general* methods have been proposed: linear cryptanalysis, differential cryptanalysis, ... Extensively used cryptographic standards – such as AES [1] – are all resistant against linear and differential attacks. In this talk, we will describe another general method – *Algebraic Cryptanalysis* – which can be used to evaluate the security of such cryptosystems.

Algebraic cryptanalysis can be described as a general framework that permits to evaluate the security of a wide range of cryptographic schemes.The basic principle of such cryptanalysis is to model a cryptographic primitive by a set of multivariate polynomial equations. The system of equations is constructed in such a way that solving the system is equivalent to recover a secret information of the cryptographic primitive (for instance, the secret key in the case of an encryption scheme). Consequently, evaluate the security of this cryptosystem is equivalent to estimate the theoretical and practical complexity of solving the corresponding system of equations. Since one of the most efficient tool for solving algebraic system over finite field is Gröbner bases [2], it is necessary to evaluate theoretically (e.g. [3]) and practically (e.g. [8]) the complexity of computing Gröbner bases over $\mathbb{F}_q$.

While it is well known that solving system of polynomial equations is NP-hard [4] in many applications, including cryptography, the polynomial systems that we have to consider are *not random* at all (see for instance [6]). Hence, it is a crucial task to identify several classes of polynomial systems that are easier to solve (or at least such that we are able to predict accurately the complexity [5]). In this

V.P. Gerdt, E.W. Mayr, and E.V. Vorozhtsov (Eds.): CASC 2009, LNCS 5743, pp. 79–80, 2009.

talk we will consider a public-key cryptosystem (namely the Minrank problem) and we will show [7] how its multi-homogenous structure can be used to predict accurately the complexity of the Gröbner basis computation. For instance, for a recommended family of parameters, we can solve the corresponding systems in polynomial time and thus break the corresponding cryptosystem.

References

1. Daemen, J., Rijmen, V.: The Design of Rijndael: The Wide Trail Strategy. Springer, Heidelberg (2001)
2. Buchberger, B.: An Algorithm for Finding the Basis Elements in the Residue Class Ring Modulo a Zero Dimensional Polynomial Ideal (German), PhD Thesis, Univ of Innsbruck, Math. Institute, Austria, English Translation: J. of Symbolic Computation, Special Issue on Logic, Math and Comp Science: Interactions 41(3-4), 475-511 (1965)
3. Bardet, M., Faugère, J.-C., Salvy, B., Yang, B.-Y.: Asymptotic Behaviour of the Degree of Regularity of Semi-Regular Polynomial Systems. In: Proc. of MEGA 2005, Eighth International Symposium on Effective Methods in Algebraic Geometry (2005)
4. Garey, M.R., Johnson, D.B.: Computers and Intractability. A Guide to the Theory of NP-Completeness. W. H. Freeman, New York (1979)
5. Courtois, N.: Efficient Zero-knowledge Authentication Based on a Linear Algebra Problem MinRank. In: Boyd, C. (ed.) ASIACRYPT 2001. LNCS, vol. 2248, p. 402. Springer, Heidelberg (2001)
6. Faugère, J.-C., Joux, A.: Algebraic Cryptanalysis of Hidden Field Equation (HFE) Cryptosystems using Gröbner bases. In: Boneh, D. (ed.) CRYPTO 2003. LNCS, vol. 2729, pp. 44–60. Springer, Heidelberg (2003)
7. Faugère, J.-C., Levy-dit-Vehel, F., Perret, L.: Cryptanalysis of MinRank. In: Wagner, D. (ed.) CRYPTO 2008. LNCS, vol. 5157, pp. 280–296. Springer, Heidelberg (2008)
8. Faugère, J.-C.: A New Efficient Algorithm for Computing Gröbner Basis without Reduction to Zero: F_5. In: Proceedings of ISSAC, July 2002, pp. 75–83. ACM press, New York (2002)